**Understanding Heartbleed vulnerability**

**What is this?**

Heartbleed vulnerability, which is also known as heartbleed bug, is a type of vulnerability that is present in the OpenSSL software library which gets its existence from inappropriate input. OpenSSL is the most famous library of open-source software. This is a type of implementation bug (CVE-2014-0160) in the software library. CVE-2014-0160 is the reference to the heartbleed vulnerability bug. CVE which is the abbreviation of Common Vulnerabilities and Exposures is the standard for Information Security Vulnerability names that are maintained and looked after by MITRE.

This vulnerability was first founded in 2014. Any individual possessing an active internet connection can make full use of this bug to extract and read the entire memory of vulnerable systems, thereby leaving no evidence of a system that is compromised. This reading in turn compromises all the secret keys which are used to recognize all the service providers and also to encrypt the traffic, the names, and passwords of the users and the actual content.

**How does this vulnerability function?**

Every time an individual visits a particular website and fills in a password, the website of the browser has to check if it's right or wrong. To do this, the browser exchanges information with the computers where all the information on the website is generally stored.

To take a real-world example, one can imagine the exchange of information as the conversation between the browser and the computer. To avoid cyber criminals and hackers from stealing and hijacking all the necessary and valuable information, different types of websites use open source software which is known as OpenSSL which is the most popular open source software to provide SSL encryption. The function of SSL is to translate all the valuable information into gibberish so that none but the browser and the organization's system will understand. Even if a hacker steals a message, it is not possible for the hacker to comprehend the gibberish and hence the confidential data and information are kept safe.

But during the checkup, there is a second parallel conversation going on which is often also called a heartbeat. When the browser is connected to the other computer, it constantly checks whether the system has fallen asleep or not. Since this conversation did not have any confidential information, it was not encrypted. But unfortunately, hackers can manipulate this request on a website that uses OpenSSL. By sending thousands and thousands of requests, these cyber criminals gain access to a lot of confidential data. But in this case, by changing the password and updating the OpenSSL in case of a website, the risk associated with this can be prohibited.

**How can this be prevented?**

Certain recommended steps can be followed to protect the server from the vulnerability. These are as follows.

1)The first and foremost step is to update the operating system, be it Linux, or windows. In addition to updating the operating system, the OpenSSL packages can also be updated.

2)After updating the system, it is necessary to check the version of OpenSSL.Version 1.0.1 is the official version that fixes this bug.

3)After updating the SSL packages and checking the versions of the OpenSSL, the old keys need to be revoked and new keys need to be introduced by a process known as rekeying.

4)Lastly, all the extra remarks have to be seen from the client’s eye and resolve as soon as possible, like changing the password, removing the cookies, etc.

**References**

1)<https://www.valencynetworks.com/articles/how-to-fix-openssl-heartbleed-vulnerability.html>

2)<https://www.synopsys.com/blogs/software-security/heartbleed-bug/>

3)<https://www.digicert.com/blog/heartbleed-openssl-fix>

4)<https://en.wikipedia.org/wiki/Heartbleed>

5)<https://geekflare.com/how-to-test-heart-bleed-ssl-vulnerabilities-cve-2014-0160/>

6)<https://www.vox.com/2014/6/19/18076318/heartbleed>

7)<https://heartbleed.com/>